Anti-Virus Comparative

Mobile Security Review 2017

Language: English
July 2017

Last Revision: 14th August 2017

www.av-comparatives.org

Table of Contents

Introduction

This report provides test reports and reviews of security products for smartphones running Google's Android operating system in version 6.0.1. The unmodified version of the operating system as provided by Google is used in order to eliminate problems due to modifications of the OS by e.g. third-party smartphone manufacturers. Amongst other things, this report aims to help readers decide whether they would benefit from the more comprehensive and sophisticated security features provided by a third-party security app.

Besides the reviews which cover the user experience of the apps, comprehensive tests on malware protection rates and battery consumption are provided as well. Additionally, a short table at the end of each product report gives an overview of any anti-theft functions included in the product. Many of the reviewed and tested apps have components which are not security-related, such as a power and memory optimizers and data backup tools.

The review mainly focuses on the security features – anti-malware, anti-theft, and privacy – and only mentions further functionalities briefly. The structure of each product report is identical, allowing readers to compare products easily.

The main purpose of a mobile security product is to protect users and their devices from potential harm inflicted by malicious apps, fraudulent mails, or phishing URLs. Readers should note that recent Android versions incorporate some basic anti-malware features. For example, Google's *Safe Browsing* API protects against malware and phishing links when the user is surfing the Internet using the Chrome browser.

Furthermore, an anti-theft component in a security app could be used to retrieve a lost or stolen phone, and/or prevent access to any personal data stored on the device. Basic anti-theft features (lock, locate, alarm, and wipe) are already provided by recent versions of Android via the Android device manager and Google's *Find My Device* function.

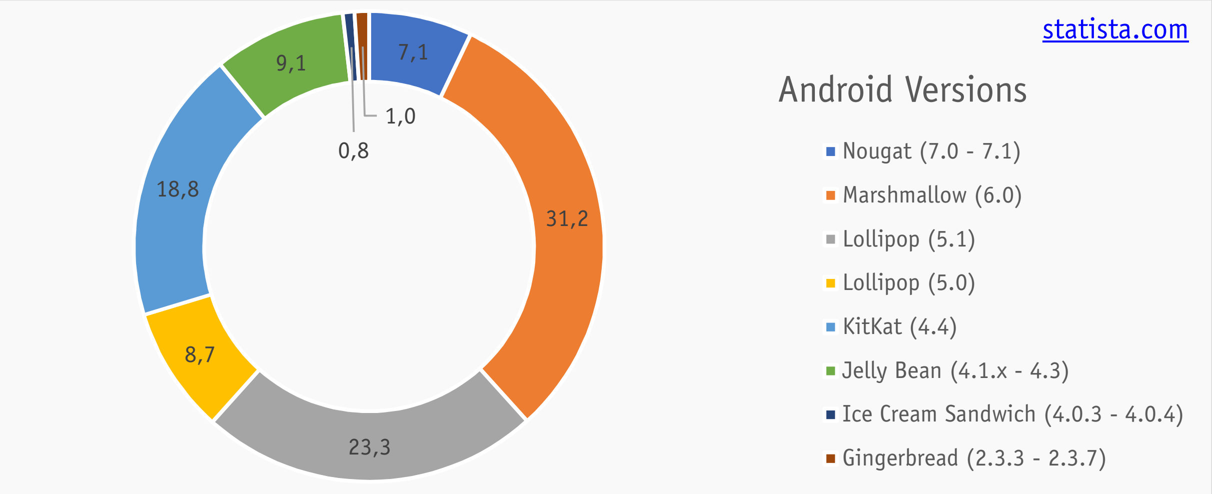
On the following pages, we provide a brief overview of the risks facing smartphone users from malware and the loss or theft of their device, and discuss the benefits of security apps. We start by recapping *Android Marshmallow*, its new permissions system, and mentioning the restrictions in the operating system that security vendors have to deal with. We will also briefly cover Google's new security service for Android called *Play Protect* which was released recently (July 2017). After that, we give a short summary of security features and their main sub-components commonly implemented in most security apps for Google Android.

At the end of the introduction, we list the participating security products, and present the results of the malware and battery drain tests. Detailed reviews of the individual products follow, in which we will shed light on the layout and usage of the features. In the table representing a product's anti-theft features, we comment on each function briefly and use the following symbols to indicate how good it worked in our tests.

✓	▬	✗
everything worked fine	minor issue(s)	major issue(s)

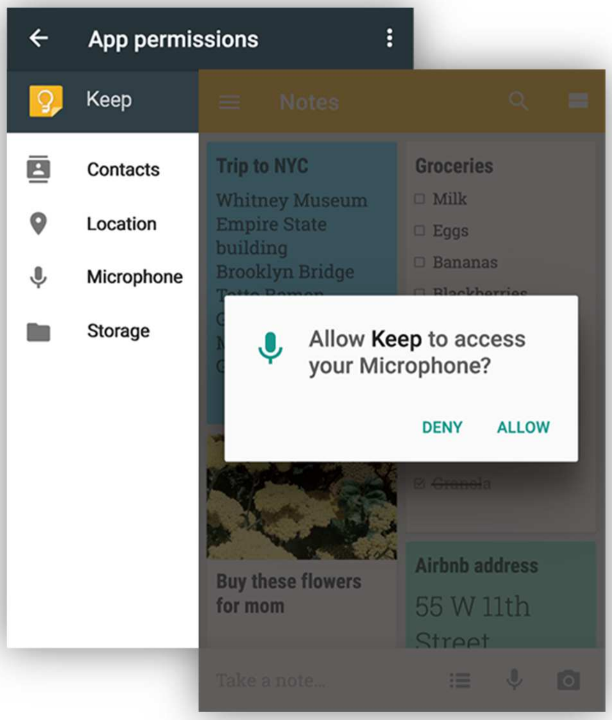
Android Marshmallow

Android version 6.0 (also known as Android Marshmallow) was officially released in October 2015. Since our last year's report, its market share increased to more than 31% as shown in the graph below[1]. Many manufacturers upgraded the operating system for their older phones and Android Marshmallow is currently running on almost every third Android device. Android 7.0 and 7.1, the recent Android versions, are only installed on a few brand-new devices (7.1%) but updates will be available for older devices gradually. Therefore, we decided to use Android 6.0.1 for this review.



The new permission-management system in Android 6.0 introduced individual post-installation and run-time permission requests where an app will ask for a specific permission the first time it needs it. This gives the user more control over the permissions granted or revoked to individual apps as shown in the screenshot on the right. Even though it may be possible to remove single permissions from an app after the installation, the app is not guaranteed to work properly. But, a well-implemented app would simply request the specific permission the next time it is required.

Additionally, with the release of the API level 23 the account management was more restricted, to enhance the security of Google Android. This means the system now denies apps permission to remove existing accounts (such as the main Google account) from the



Allow **Keep** to access your Microphone?

DENY ALLOW

[1] https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

phone; an app can only delete accounts it has created itself. Security products developed for previous Android versions used this feature to perform a data-only wipe. Such a wipe has the advantage that all sensitive data can be deleted from the phone without losing the ability to control the anti-theft features provided by the installed security app.

It should be noted that all of this relates to a rather theoretical problem. As mentioned in previous reports, if a phone has been encrypted and set up properly with a lock screen using a PIN, strong password, or custom pattern, it is virtually impossible for a thief to retrieve any data from it.

Google Play Protect

In May 2017, Google announced its new built-in malware protection for Android, which checks apps and .APK files when they are downloaded from the Google Play Store or third-party sources. It is a redesign of the existing *Verify Apps,* which only checks apps installed outside the Play Store. With this enhancement, Google constantly monitors the device and all the user's data with the aim of keeping them safe[2]. Play Protect scans all installed apps and the device for suspicious findings. Scans no longer run only in the background, but can be manually triggered by the user as well; the current status is clearly shown in the Play Store. It will also notify the user about the device's security and any security risks found in more detail.

If a potentially harmful app is detected, it will immediately be prevented from running. Google Play Protect will then display a warning and a suggestion to the user to uninstall the app. Google is gradually delivering the update for the Play Store to all Android devices running Play Services 11 or later. The service itself can be found under *Settings* -> *Google* -> *Security* -> *Verify Apps,* and shows a slight modification of the previous Verify Apps screen. This does not detract significantly from the device's performance, as Play Protect uses cloud connectivity for its analysis, and is aided by Google's machine learning to monitor around 50 billion apps each day (currently). It goes hand in hand with *Find My Device* and *Safe Browsing,* and will bundle all three functions (malware scanner, device loss, and safe browsing) in the future.

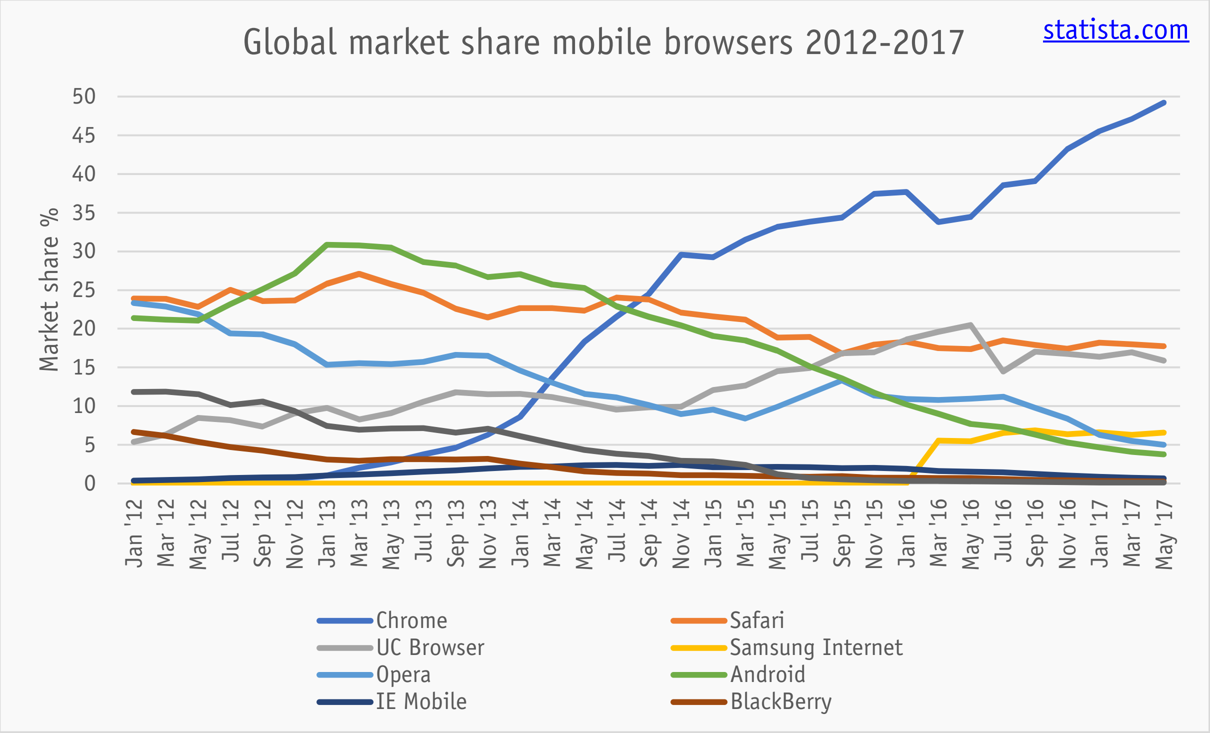
[2] https://www.android.com/play-protect/

Security Features

In this section, we give a short overview of common security-related components found in most security products for Google Android.

The most obvious component of a mobile security app is the malware scanner. This protects the user against the inadvertent installation of malicious apps on his/her device. Similarly to anti-virus programs for Microsoft Windows, mobile security apps for Android use a number of different protection features. The *real-time scanner* checks new apps during the setup process. This prevents the device being compromised by the installation of a malicious program. *On-demand scanners* search the whole device (internal storage and/or external SD card) for any malicious applications that are already installed, or downloaded APK files that have not yet been run. As with Windows desktop security applications, keeping malware definitions up to date is a critical factor in effective protection. Some vendors offer more frequent updates with their paid premium versions than with the corresponding free versions. We noticed that many of the tested products offer a cloud-assisted malware scanner to ensure the app has access to the very latest definitions. Updates are either retrieved automatically by the app after a certain time or can be downloaded by the user manually.

A major component in various security apps is the anti-theft module. It is designed to execute commands on a target device that has been lost or stolen. As mentioned in previous sections, Android 6.0 includes core anti-theft features such as remote device lock, location, wipe, and an alarm sound. Many of the security products we tested extend this base functionality with additional features such as taking pictures of the thief using the built-in front and/or back camera of the device, location tracking, or automatic notification in the event of a SIM card change. Usually, the anti-theft components are controlled via a web interface, but several apps also support text-message commands. The latter have the advantage that they work even if no Internet connection is available, but they are less convenient to use. For example, if the Android OS is not appropriately configured by the user, text messages are shown shortly before locking the screen or on the lock screen itself as notifications. Therefore, texts containing e.g. the unlock code could be read by a thief. With Android 4.4 and later, app developers are no longer able to programmatically delete text messages as they arrive. Hence, they can no longer prevent the text messages used for their commands being seen on the screen when they appear. To get around this issue, some manufactures developed a custom binary SMS system. This function is provided by the anti-theft feature of the security app itself meaning the same app has to be installed on the friend's/relative's phone used to send the anti-theft SMS commands.



Several security products offer browser protection which prevents the user from unintentionally downloading malicious apps or accessing phishing websites while surfing the Internet. Some apps support a variety of different browsers, including those made by third-party app developers. This is an important question as many smartphone users like to use their preferred browser on their smartphones. In our last year's report, we criticized the fact that some of the tested products only offered browser protection for the standard Android browser. This restriction seemed quite inadequate, because the stock browser was removed from Android 4.4, and there has not been a standard Android browser in the OS versions since then. The products tested in this report support protection and web security for at least Google Chrome, which we used in our test scenario, and Mozilla Firefox. The graph above[3] shows the market share of mobile browsers as at May 2017. Almost 50% of smartphone users surf the Internet using Google Chrome. Apple's Safari browser follows on the second place with ~18% and the Android browser still occupies a share of 3.75% with a decreasing trend.

A privacy advisor is also included in many of the tested products. It scans the installed apps not for malicious behavior but for possible privacy violations. In other words, apps are analyzed for uncommon, unnecessary, or inappropriate app permissions such as access to contacts, GPS position, or the Internet, which could lead to the user's private sphere being breached. As a result of this scan, some security products advise the user to uninstall any apps that have given themselves such unneeded permissions.

[3] https://www.statista.com/statistics/263517/market-share-held-by-mobile-internet-browsers-worldwide/

Products tested

The products included in this year's test and review are listed below. The latest products[4] were taken from major app stores like Google Play at the time of the test (July 2017). After the product review, manufacturers had the opportunity to fix any flaws we found. Any problems that have already been solved are noted in the report.

Vendor	Product Name	Version	Features
AI Max Dev Labs	Security Antivirus – Max Cleaner	1.0.0	● ○ ● ● ● ○
Alibaba	Ali Money Shield	5.5.0	● ● ○ ● ● ○
Avast	Mobile Security & Antivirus	6.1.3	● ● ● ● ● ○
Avira	Antivirus Security	5.0.2	● ● ● ● ● ○
Bitdefender	Mobile Security & Antivirus	3.2.96	● ● ● ● ○ ○
ESET	Mobile Security & Antivirus	3.6.46	● ● ● ● ● ○
Kaspersky Lab	Internet Security	11.14.4	● ● ● ● ● ○
McAfee	Mobile Security	4.9.1	● ● ● ● ● ●
Tencent	WeSecure	1.4.0	● ○ ○ ○ ● ○
Trend Micro	Mobile Security	8.2.4	● ● ● ● ● ○

Symbols

To give an easy overview of the features of a product, we are introducing symbols like the we already use on our website. At the beginning of every report, you will see all these symbols; those in orange represent features the product has, while those in grey represent features that are not included.

Anti-Malware	●	includes a feature to scan against malicious apps
Anti-Theft	●	includes remote features in case the smartphone gets lost or stolen
Safe-Browsing	●	includes a web filtering feature to block dangerous sites
App Audit	●	includes features to audit installed apps
Anti-Spam	●	includes features to block unwanted calls and/or SMS
Backup	●	includes a feature to backup files on the smartphone

[4] A comprehensive overview of the mobile security products available on the market can be seen on our website: http://www.av-comparatives.org/list-mobile/

Overview

The perfect mobile security product does not yet exist. As with Windows products, we recommend drawing up a short list after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days; this should make the decision easier. Especially with Android security products, new versions with improvements and new functions are constantly being released. By participating in this test, the manufacturers have shown their commitment to providing customers with quality security software. As this report shows, we have found some degree of malfunction in some of the tested products. The manufacturers of the affected products have taken these problems seriously and are already working on solutions. 8 of this year's participants qualify for our "Approved Mobile Product" award, by providing solidly working core functions and solid malware protection.

X **AI Max Dev Labs** Security Antivirus – Max Cleaner is a convenient app which comes with the most important security features. Unfortunately, it fell somewhat short of the malware protection level required for certification.

Alibaba Ali Money Shield is an easy-to-use product, clearly focused on security and payment protection.

Avast Mobile Security and Antivirus offers well-implemented features for almost any use case.

X **Avira** Antivirus Security is in principle a well-designed app, but does not reach certification level this year, as it did not quite meet the minimum malware protection level.

Bitdefender Mobile Security and Antivirus is an easy-to-use product which offers great protection against malware as well as a mature anti-theft feature.

ESET Mobile Security and Antivirus is a well-developed security application for Android, including a variety of different security and anti-virus features within a neat graphical interface.

Kaspersky Internet Security for Android is a comprehensive mobile security app for users who want all their security features in a single application.

McAfee Mobile Security provides a great security product with good malware detection and a comprehensive anti-theft component.

Tencent WeSecure represents a basic, lightweight anti-virus application and offers some useful tools in addition.

Trend Micro Mobile Security for Android is a comprehensive app that provides an advanced security concept and additional, helpful features.

Protection against Android malware

Methods of attacking mobile devices are getting more and more sophisticated, with fraudulent applications attempting to steal users' data or money. To reduce the risk of this happening, follow the advice given here. Only download apps from official app stores like Google Play or stores of reputable app makers, and avoid third-party stores and side-loading[5]. Irrelevant access rights are another indicator of untrustworthy apps. For example, an app that counts the steps the user takes every day has no need to access the phone book or call log. Of course, even if an app behaves like this, it does not necessarily mean that it is malicious, but it makes sense to consider whether it is genuine and worthy of use. A quick look at the reviews in the app store before installing an app is also a guide; avoid apps with predominantly bad or dubious reviews. Rooting the smartphone may gain the user more functionality on the phone, but also increases the risk that malicious apps will take control of the device. Furthermore, it is not legally clear-cut whether the warranty is still valid if the phone is rooted. With some manufacturers, the warranty will be considered null and void. Public Wi-Fi networks without appropriate security are opportunities for malware to steal or comprise sensitive personal data. Whenever connecting to a public Wi-Fi hotspot e.g. in a coffee shop, be aware of the security risks when sharing information. Never expose data (user credentials, Wi-Fi passwords, bank/credit card information, etc.) that shouldn't be shared with others. This doesn't only hold for Android devices but also for other portable devices from different manufacturers.

How high is the risk of malware infection with an Android mobile phone?

This question cannot be answered in one sentence as it depends on many different factors. In western countries where official stores such as Google Play are mostly used, the risk is much lower than in many Asian countries, especially China. Many rooted phones and third-party app stores can be found there, increasing the chance of installing a dangerous app. In many parts of Asia, the smartphone is also used as a replacement for the PC, and is frequently employed for online banking. Nowadays, banking apps have also become popular in Europe and the USA. There is a high risk involved in receiving the TAN code on the same phone that is used to carry out the subsequent money transfer. In western countries, assuming you stick to official app stores and don't root your phone, the risk of the smartphone becoming infected is currently relatively low, in our opinion. However, we must point out that "low risk" is not the same as "no risk". In addition, the threat situation can change quickly and dramatically. It is better to be ready for this and to install appropriate security software on the smartphone. Currently, we would say that protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

AVC UnDroid Analyzer

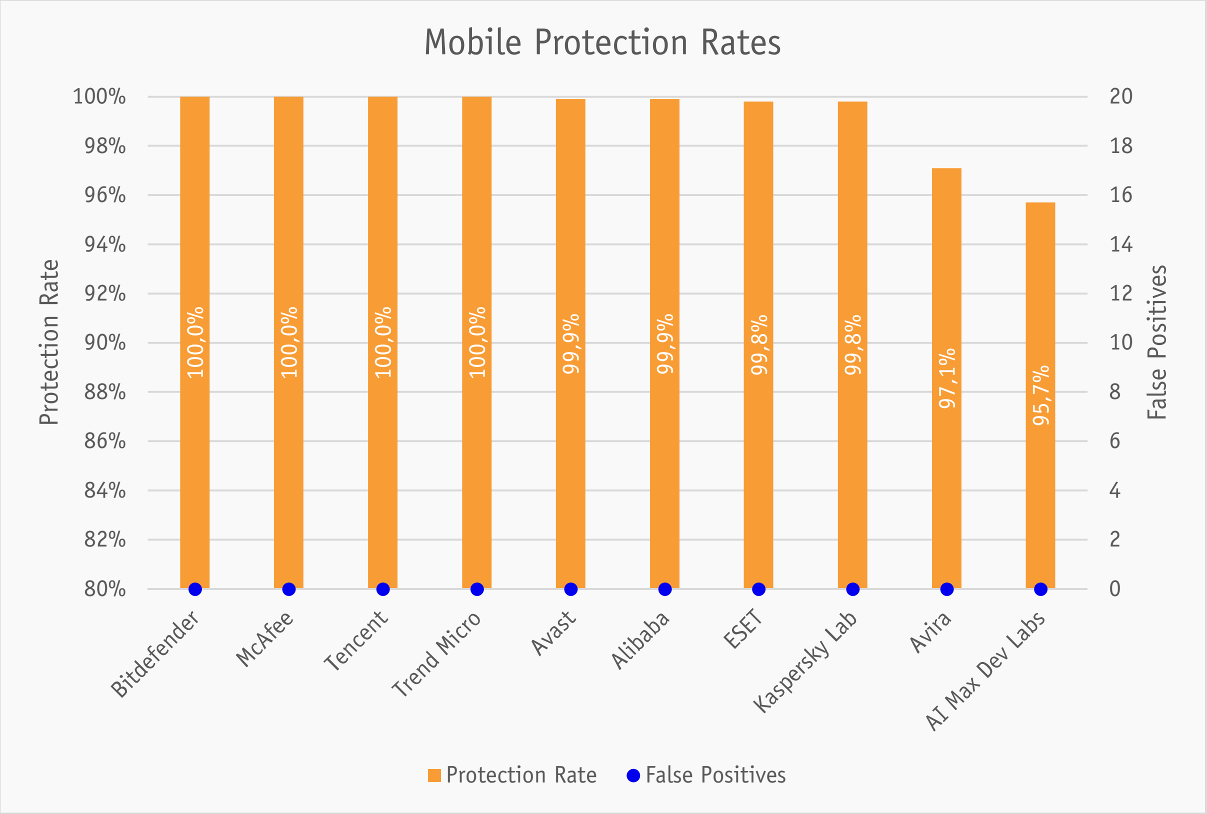
At this point, we would like to recommend *AVC UnDroid*, our malware analysis tool, which is available free to all users. It is a static analysis system for detecting suspected Android malware and adware and providing statistics about it. Users can upload APK files and see the results in various analysis mechanisms.

We invite readers to try it out: http://www.av-comparatives.org/avc-analyzer

[5] http://en.wikipedia.org/wiki/Sideloading

Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **4,081** malicious applications, to create a representative test set. So-called "potentially unwanted applications" (PUA) were not included. The security products were updated and tested on the 11th July 2017. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of APK files. An on-demand scan was conducted first. After this, every undetected app was installed and launched. We did this to allow the products to detect the malware using real-time protection. A false-positives test was also carried out by downloading 500 popular apps from various popular third-party app stores. The results can be seen below (sorted by Malware Protection and number of False Alarms).



As can be seen above, the protection rates against real Android malware are quite high, averaging just over 98%. This might be due to the increasingly aggressive detection by app reputation for apps that are not on whitelisted app stores, but also because many of the participants in our test are leading mobile security vendors with good protection rates.

Mobile Protection Rates		
	Protection Rate	False Positives
Bitdefender, McAfee, Tencent, Trend Micro	100.0%	0
Avast, Alibaba	99.9%	0
ESET, Kaspersky Lab	99.8%	0
Avira	97.1%	0
AI Max Dev Labs	95.7%	0

Battery Drain Test Results

As in our previous reports, we measured the additional power consumption of an installed mobile security product. Testing the battery usage of a device might appear to be very straightforward at first glance. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones, the usage patterns of different users are very varied. Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users who take advantage of all the possible functions in the device and traditional users who merely make and receive phone calls.

The test determined the effect of the security software on battery use for the average user. The following daily usage scenario was simulated:

- 30 minutes telephony
- 82 minutes looking at photos
- 45 minutes surfing the Internet using the Google Chrome browser
- 17 minutes watching YouTube videos using the YouTube app
- 13 minutes watching videos saved on the phone itself
- 2 minutes sending and receiving mails using the Google Mail client
- 1 minute opening locally saved documents

In our test, we found that most mobile security products have only a minor influence on battery life, as is outlined in the table below.

Battery Drain Results	
AI Max Dev Labs	▰▰▰▰
Alibaba	▰▰▰▰
Avast	▰▰▰▰
Avira	▰▰▰▰
Bitdefender	▰▰▰▰
ESET	▰▰▰▰
Kaspersky Lab	▰▰▰▰
McAfee	▰▰▰▱
Tencent	▰▰▰▰
Trend Micro	▰▰▰▱

▰▰▰▰	up to 3%
▰▰▰▱	3 to 8%
▰▰▱▱	8 to 15%
▰▱▱▱	15 to 25%
▱▱▱▱	more than 25%

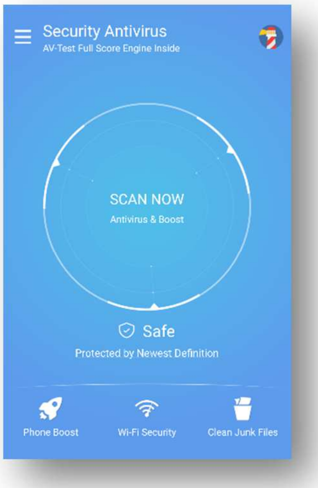
In general, we were able to give the tested security suites high marks. Two products in this year's test showed a slightly increased battery drain: **McAfee** and **Trend Micro**.

AI Max Dev Labs

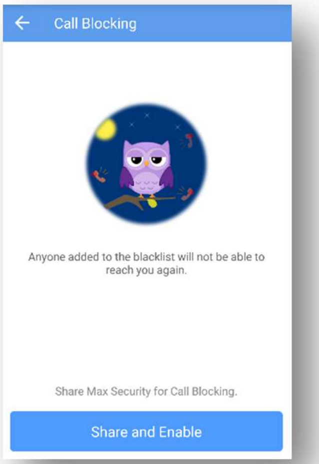
Security Antivirus – Max Cleaner
1.0.0

Introduction

This product mainly concentrates on the anti-virus functions, while also offering features like App Lock, Safe Browser, Call Blocker, or Wi-Fi Scanner. It only comes in a free version, which has all features available by default.



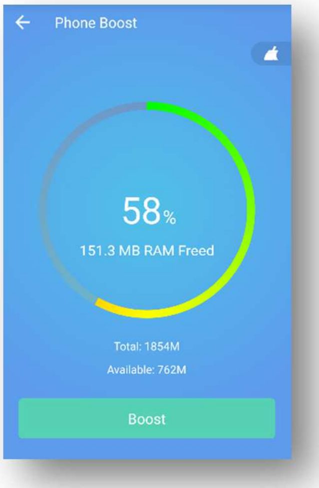
Security Antivirus
AV-Test Full Score Engine Inside



Call Blocking

Anyone added to the blacklist will not be able to reach you again.

Share Max Security for Call Blocking.



Phone Boost

58%
151.3 MB RAM Freed

Total: 1854M
Available: 762M

Usage

After installing the application on the device, the user is immediately led to the home screen. Most of the features are displayed on the bottom or in a sidebar.

Anti-Ransomware

This tool will detect and delete files or apps already installed on the phone. It also provides a feature where whenever the screen is locked, the user has to activate and deactivate the screen three times to get help. In addition, the user is requested to set a pattern which can be changed to a code later and to decide what information will be shown on the lock screen. Everything, nothing, or no sensitive content are the options.

Safe Browsing

After activation, the feature is ready to use. Unfortunately, when we visited known harmful phishing websites with multiple browsers in our test, only 1 out of 15 of these were detected.

Wi-Fi Security

This feature scans the current and other available networks for potential threats. After the scan is completed, the connection speed is shown, as well as further information about the network (such as IP and MAC address).

App Lock

This tool requests the user to draw a safety pattern (that can be changed to a code later) to unlock the selected apps afterwards, as well as to choose a security question. The apps locked by default in our test were Google's apps Gmail, Photos, Google+, Hangouts, and Chrome, which indicate privacy issues.

Call Blocking

This component is only available after sharing/recommending the app via a text message or an email to a friend or contact.

With this feature, the user is able to block phone numbers or contacts. Unfortunately, it is not possible to block unknown or hidden numbers, while blacklisting is very inconvenient (only single numbers, not lists or groups, can be added). The phone disconnects the call from a blocked number after ringing once.

Task Bar

The app also provides a Task Bar in the Android notification area, to easily and quickly access important features like the anti-virus and Wi-Fi scanner, Phone Boost, and the device's flashlight.

Conclusion

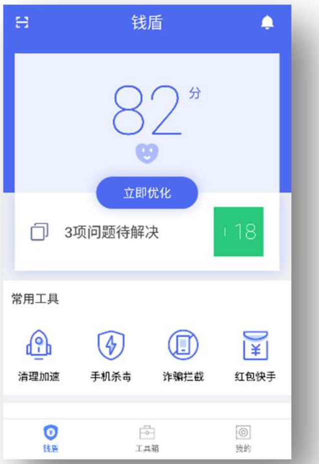
Security Antivirus – Max Cleaner is convenient to use and the user has most of the important security features in one app. Even though an anti-theft function and a functional browser protection would be nice, all other features worked as expected.

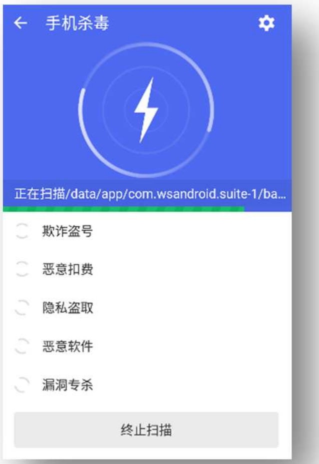
Alibaba

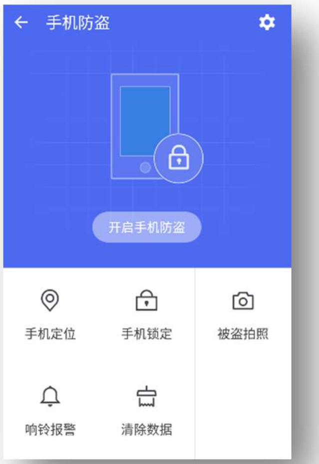
Ali Money Shield
5.5.0

Introduction

The Ali Money Shield is a free security product which includes performance and various security components, but clearly focuses on providing protection for users with a Taobao account. The app is only available in Chinese language.







Usage

After an initial setup, the user is directed to the main screen, which is divided into three parts. The “Money Shield” shows the score of the quick security check, and useful tools like a storage cleaner, AV scanner, and call blocker. The “Tool Box” contains further components for security and privacy purposes. “My Safe Box” displays information about the user’s Taobao account and enables access to different app settings.

Security Check

The quick security check rates the device’s security status according to Alibaba’s scoring rules, and displays its result (health points) on top of the “Money Shield” tab. Users can earn additional health points by surfing the internet more securely (via VPN), activating their Taobao account protection, conducting a deep AV scan, and protecting themselves against privacy and security risks from unsecure Wi-Fi networks and applications. Furthermore, the security check is performed on each start of the app.

Anti-Virus

The AV Scanner is accessible on the “Mobile Shield” tab and part of the common tools. It provides a quick scan, which scans all installed apps by default. The settings can be changed to perform a full system scan of all files. AV database updates are done automatically.

Anti-Theft

Only users with a valid Taobao account can use the theft protection feature. For this reason, the app requests administrator permissions for the device. The user can then send anti-theft commands via a neat web interface on *qd.alibaba.com*, which includes locking/unlocking the device, sounding an alert, locating the device, and wiping personal data. Furthermore, the app can take pictures of a potential thief, using the device’s front- and back-facing cameras, which are then displayed within the web interface.

Fraud & Nuisance Blocker

Besides a simple storage cleaner to free and optimize the device's storage, the app comes with a call and message blocker. The user can white- or blacklist certain numbers or contacts to protect him/herself against unsolicited sales calls and fraud text messages.

Tool Box

The Tool Box offers a large collection of useful tools like a Wi-Fi scanner, an app locker, and a monitoring tool which shows phishing site detections and statistics about counterfeit links (limited to mainland China). In addition, the anti-theft component can be found here, as well as a payment guard, a software uninstaller, and a notification assistant among many other tools. The user can also access the Ali app store, and Ali 110 to report Taobao-related problems such as hacked Taobao accounts.

My Safe Box

On this tab, users can find the app settings, add and get information about their Taobao account, and verify themselves as the rightful owner of the account. For each authentication step done in-app, a text message is sent to the registered mobile phone number.

Task Bar

One special feature that comes with this app is the "Ali Taskbar" in the Android notification area. From here, the user has easy access to a smartphone tuning tool, a "safe" OCR scanner, clean-up functions, and the flashlight. Further, the number of nuisance calls and text messages that have been intercepted by the app is displayed.

The Ali Spaceship

After the installation of the app, a tiny circular object (we call it "spaceship") is placed on one side of the mobile desktop. The user can drag the spaceship to the middle of the screen which then performs a quick check-up and clean-up of the device.

Conclusion

Ali Money Shield is an easy-to-use product with a clear focus on security and payment protection. It provides a bunch of useful tools from device optimizers and cleaners up to a call/message blocker and AV-related features. Due to the simple design and the meaningful placement of its components, the app does not seem overloaded with features. However, we recommend adding a deinstallation password to the theft-protection functionality.

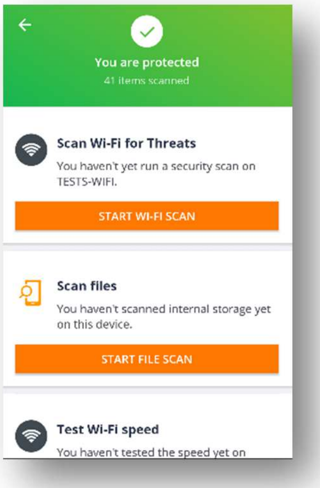
Anti-Theft Details		
Commands Web		
Alarm	✓	Sounds an alarm on the device.
Locate	✗	Limited to mainland China and does not work for other countries.
Lock	✓	Locks the device with a 6-digit password.
Wipe	−	Deletes contacts, call logs, and pictures only on internal storage.
Additional Features		
Face Cam	✓	Takes pictures with the front and back camera to identify the thief.

Avast

Mobile Security & Antivirus
6.1.3

Introduction

Avast offers a comprehensive app with all the important security features that will give the user a good level of overall protection. Amongst many other, non-security related features, the application provides malware scan, anti-theft, Wi-Fi security, app lock, app permissions, call blocker, and a firewall feature. The latter is only available to users with a rooted device.

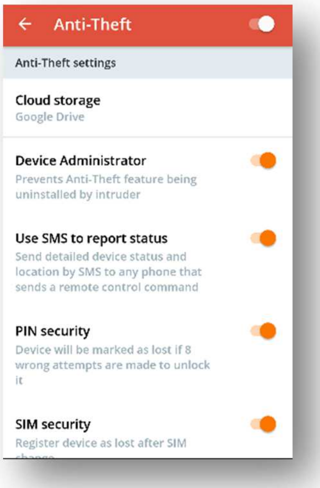


You are protected
41 items scanned

Scan Wi-Fi for Threats
You haven't yet run a security scan on TESTS-WIFI.

Scan files
You haven't scanned internal storage yet on this device.

Test Wi-Fi speed
You haven't tested the speed yet on



Anti-Theft

Anti-Theft settings

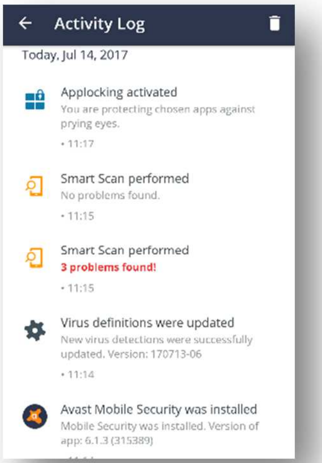
Cloud storage
Google Drive

Device Administrator
Prevents Anti-Theft feature being uninstalled by intruder

Use SMS to report status
Send detailed device status and location by SMS to any phone that sends a remote control command

PIN security
Device will be marked as lost if 8 wrong attempts are made to unlock it

SIM security
Register device as lost after SIM



Activity Log

Today, Jul 14, 2017

Applocking activated
You are protecting chosen apps against prying eyes.
• 11:17

Smart Scan performed
No problems found.
• 11:15

Smart Scan performed
3 problems found!
• 11:15

Virus definitions were updated
New virus detections were successfully updated. Version: 170713-06
• 11:14

Avast Mobile Security was installed
Mobile Security was installed. Version of app: 6.1.3 (315389)

Usage

After installing the app and accepting the EULA, the user can decide if he/she wants to stay on the free version or upgrade to the pro version directly, which costs €7.99 for a year or €1.99 for a monthly subscription. Afterwards, the home screen of the app shows up.

Anti-Virus

The malware scan is kept very simple as all options to adjust the scan process are hidden in the app settings. There, the user can decide if files in the internal storage should be scanned for any threats in addition. Scheduled scans can be set for any day and time and detection of PUAs as well as the protection against applications and data with a poor security level can be enabled.

Anti-Theft

The feature provides both web and text-message commands. The initial setup requests the user to set up a code which is required to send the SMS commands and to unlock the screen. Pictures taken of the culprit, as well as recorded audio and backup data, can be found and downloaded via the web interface or optionally uploaded to Google Drive. A more convenient way to send the text-message commands is the SMS Remote Control. This feature allows the user to select anti-theft commands from a list, and send them to a target phone which also must have the Avast app installed. Furthermore, it provides a neat user interface, therefore the user does not need to remember and type in any command by hand.

Wi-Fi Security

This tool monitors currently connected Wi-Fi networks and other available networks for threats, and is able to establish if they are safe. After a test, more detailed information and the connection speed is shown on the screen.

App Locking

This feature protects selected apps from unauthorized access. The user has to enter the previously set PIN to open the protected app. Alternatively, an unlock-pattern can be used.

Call Blocker

The call blocking feature allows the user to add all unknown numbers to the blacklist (manually or from the contacts), and can further block all hidden numbers. The component worked as expected, and was able to suppress the incoming call without even ringing once (which was a minor fault in the last year's test).

App Permissions & Firewall

All installed apps are categorized into three permission groups: high, average, and low. The user can see detailed information about which permissions are granted to which app.

Avast offers a firewall for Android devices. However, this feature requires root access to the device which is not present in our test scenario. Hence, we skipped this feature.

Conclusion

Avast provides an app with a wide range of features and a user-friendly interface. The tools function well and the establishment of the in-app SMS Remote Control is really convenient. The message exchange between the two phones happens behind the scenes and the user receives no notifications as it is typical for normal text-message commands.

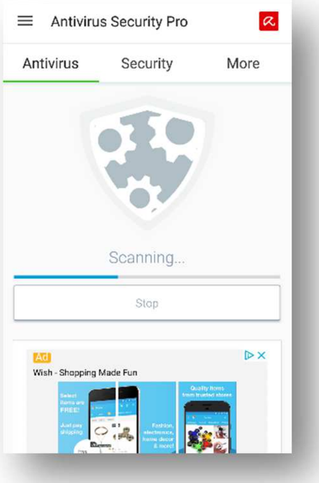
Anti-Theft Details		
Commands Web		
Locate / Track	✓	Displayed on *Google Maps* Map.
Mark as Lost	✓	Triggers configured actions like tracking, lock, siren,…
Forwarding	✓	Allows to forward all incoming calls and SMS to a given number.
Siren	✓	
Lock	✓	
Wipe	–	Triggers a factory reset. External storage is wiped but files can be restored.
Launch Anti-Theft	✓	Opens Anti-Theft user interface on device.
Record Audio	✓	Records audio for a predefined duration of 1-5 minutes.
Take Picture	✓	Takes a picture with the front or back camera. Optional: The camera is triggered when the screen is turned on.
Get data	✓	Allows fetching data (calls, SMS, contacts) from the device. We found it quite hard to find the fetched data.
Initiate Call	✓	Allows calling a given (in web interface) phone number.
Show Message	✓	Allows user to send a single message which is shown as popup.
Commands SMS		
Message	✓	SMS commands are sent from within the app' SMS Remote Control. This enables the usage of binary SMS which can't be read on the receiving phone. To get SMS answers from the receiving phone, SMS responses have to be explicitly activated. In our test, all commands worked as expected. Only the behaviour of the locate command was strange as the evaluated location will not be sent back to the phone who triggered the call but rather sent to a "friend's" number, which can be set in the advanced settings.
Mark as Lost/Found	✓	
Lock	✓	
Siren	✓	
Locate	✓	
Call	✓	
Forward	✓	
Wipe	–	
Additional Features		
SIM Change Protection	✓	Sets the phone status to lost.

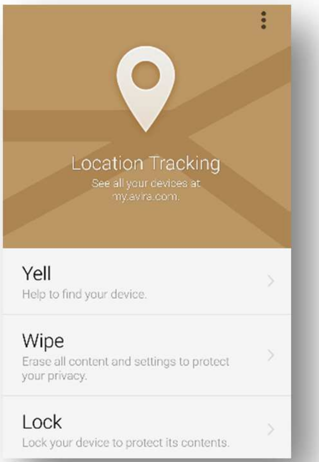
Avira

Antivirus Security
5.0.2

Introduction

Avira provides a comprehensive and nicely developed product which is available in a free and pro version. The free version provides an anti-theft feature, Security Safeguard, Privacy Advisor, and Call Blocker. Pro adds more-frequent database updates and Secure Browsing. Further functions like App Lock+ and a Password Manager are offered in separated apps.

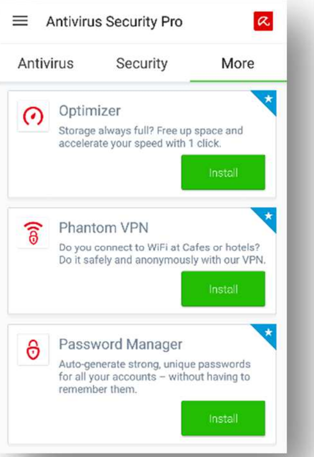



Location Tracking
See all your devices at my.avira.com.

Yell
Help to find your device.

Wipe
Erase all content and settings to protect your privacy.

Lock
Lock your device to protect its contents.



Optimizer
Storage always full? Free up space and accelerate your speed with 1 click.
Install

Phantom VPN
Do you connect to WiFi at Cafes or hotels? Do it safely and anonymously with our VPN.
Install

Password Manager
Auto-generate strong, unique passwords for all your accounts – without having to remember them.
Install

Usage

After installation, the application gives the user a brief overview of the functions the app has to offer. The two main features are Anti-Virus and Security. Most of the functions are only available after creating an account, so we recommend doing so beforehand.

Anti-Virus

The app provides a one-click scan that can be further customized in the settings. It is not shown what was scanned; only the number of files and if something was found. In the settings, the option for scanning the device for adware, potentially unwanted applications and riskware can be enabled/disabled. In addition, the user can decide if the scan should start when a USB cable is unplugged or storage is mounted. A scan schedule can also be set.

Anti-Theft

The anti-theft function supposedly consists of four features: Locate, Yell, Lock, and Wipe. In-app, only the Yell command can be executed. The others are available in the web interface We were initially not able to test most of the anti-theft features, because their controls were not provided in the web interface. The only option available was the *Family Locator* which allows the user to locate the phone on demand, and shows its location in Google Maps. After we reported the missing commands to Avira, they added the Lock/Unlock and Yell functions. Further tests showed that the device can be locked and unlocked, but neither the required message nor the optional phone number were displayed on the lock screen. After pointed out, they fixed this issue too. Furthermore, the Yell feature works now and sounds the alarm for 20 seconds. The wipe feature is still not available. Avira have told us that they are working on an enhanced version.

Additional Features

Other functions that are included in the app are Privacy Advisor, which rates the installed apps according to the number of permissions they access; a Secure Browsing function that protects the user from harmful websites while surfing; and a Call Blocker for blacklisting unwanted callers.

Conclusion

Avira Antivirus Security is essentially a well-developed, comprehensive anti-virus application which provides effective protection against malware, even though using some of the features can be a bit difficult. There are major issues with the anti-theft component in the web interface, which prevented us from testing it in detail.

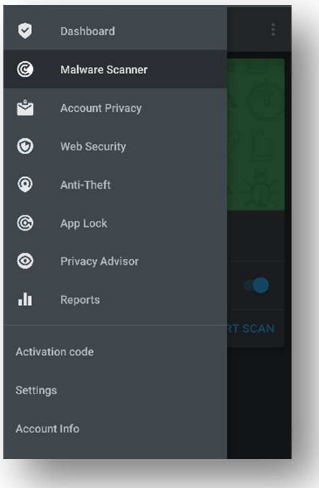
Anti-Theft Details		
	Commands Web	
Locate	✓	Displayed on *Google Maps* Map.
Yell	✓	Plays a sound for 20 seconds.
Lock	✓	Locks the device with a 4-digit PIN and shows a message on the lock screen. Optional: Call the phone number entered in the web interface.
Wipe	✗	Not available although provided in the app.
Device Report	✓	Gives available information about the phone like IMEI and device model.

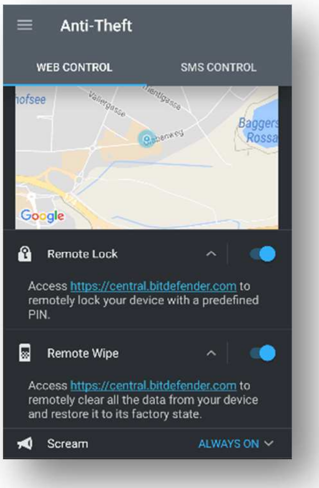
Bitdefender

Mobile Security & Antivirus
3.2.96

Introduction

Bitdefender Mobile Security and Antivirus provides the user with a well-developed and easy-to-handle app that can be bought for €9.99 per year. As well as the Malware Scan, Account Privacy, and Web Security, the app supports Anti-Theft, App Lock, Privacy Advisor, and Report functions.



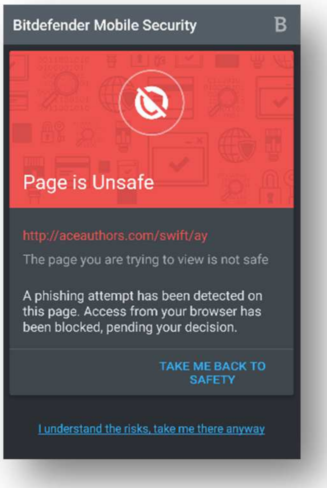


Remote Lock

Access https://central.bitdefender.com to remotely lock your device with a predefined PIN.

Remote Wipe

Access https://central.bitdefender.com to remotely clear all the data from your device and restore it to its factory state.


Bitdefender Mobile Security
Page is Unsafe

http://aceauthors.com/swift/ay

The page you are trying to view is not safe

A phishing attempt has been detected on this page. Access from your browser has been blocked, pending your decision.

TAKE ME BACK TO SAFETY
I understand the risks, take me there anyway

Usage

After the initial installation, the user agrees to the EULA by signing in with a Bitdefender account, and thereby gets a 14-day trial of the pro version. The app recommends starting with a full scan straight away.

Malware Scanner

The feature scans the device for malicious software; the user is provided with very few options. He/she can only decide if the storage should be scanned or not. As information, Bitdefender states that all new and updated apps will be scanned automatically. After the scan is completed, the app displays a short summary of the process.

Anti-Theft

After the user grants the app the rights of a device administrator, a secure PIN (4-8 digits) has to be defined. Bitdefender offers all core components for Anti-Theft: Remote Locate, Lock, Wipe, and Siren. The anti-theft features are controlled via a well-designed web interface or SMS commands. We note that the latter can be sent from any phone, except the Wipe command which can only be successfully triggered by a predefined (trusted) number. A SIM change component is included as well, which alerts the trusted number via SMS whenever the SIM card is changed. The "Snap Photo" function takes a picture of the thief, using the device's front camera, which will then be displayed in the web interface.

Web Security

This protects the following supported apps from accessing phishing websites and other potentially dangerous websites: Chrome, Firefox, Opera, Opera Mini, Dolphin, Facebook, and Facebook Messenger. The user can ignore the warning and access the website at his/her own risk by tapping the corresponding link in the warning page. During our tests, everything worked as expected.

App Lock

App Lock protects the user's privacy by locking sensitive apps and keeping them safe. There are different lock modes from which the user can decide according to his/her interests: Lock every time, unlock until screen is turned off, or re-enter the app without a password for the next 30 seconds. The previously established PIN is required for unlocking protected apps. Alternatively, the fingerprint can be used on supported devices. A "safe environment" can be set by declaring the current Wi-Fi network as trusted, which will unlock all the protected apps.

Account Privacy

Account Privacy helps to detect any data leakage in the provided and verified e-mail accounts used for making online payments, shopping, or signing in different apps or websites. If leaks occur from any account, Bitdefender notifies the user and recommends changing the password as soon as possible.

Privacy Advisor

This feature shows which installed apps requires which permissions on the device. It also gives a rating of the privacy status with its own "Privacy Score", and allows the user to uninstall apps.

Conclusion

Bitdefender Mobile Security and Antivirus provides good malware protection and a variety of security features in a neat and clear user interface. The application worked very well in our tests and seems to be mature. A small security issue which may be solved in future releases is the absence of the Uninstall Protection.

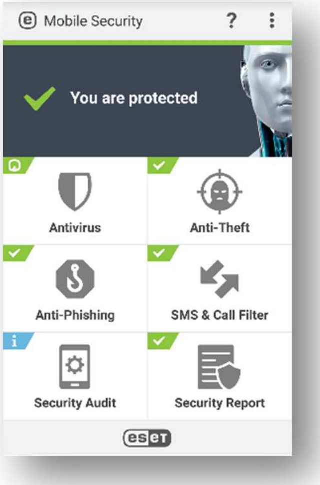
Anti-Theft Details		
Commands Web		
Locate	✓	Displayed on *Google Maps* Map.
Send Message	✓	Message can be displayed on screen. Optional: Alarm sound.
Lock Device	✓	Locks the device with the Android lock screen. The PIN is set in the web interface.
Wipe Device	▬	Triggers a factory reset. External storage is wiped but files can be restored.
Commands SMS		
Locate	✓	Link to *Google Maps* is sent.
Lock	✓	Locks the device with the Android lock screen. The user can explicitly hide the SMS preview in the notification area via the app's anti-theft feature.
Wipe	▬	As for the corresponding web command; only allowed by the trusted number/contact.
Scream	✓	
CallMe	✓	Dials the phone number from which the command was sent with the speaker turned on.
Help	✓	Sends the usable commands.
Additional Features		
SIM Change Notification	✓	Sends a SMS to the trusted number whenever the SIM card is changed.
Snap Photo	✓	Takes a picture of the thief using the device's front camera on failed unlock attempts and uploads it to the web interface.

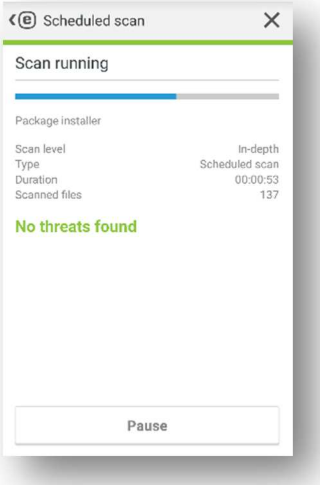
ESET

Mobile Security & Antivirus
3.6.46

Introduction

ESET Mobile Security and Antivirus is an easy-to-use application that provides a wide range of protection features. The user gets a 30-day trial of the premium version, afterwards he/she can decide on upgrading permanently or staying with the free version. Besides Virus Scans and a Security Report option, the premium version provides automatic updates as well as additional features like Scheduled and On-charger scans, Proactive Anti-Theft, Anti-Phishing, SMS & Call Filter, and Security Audit.



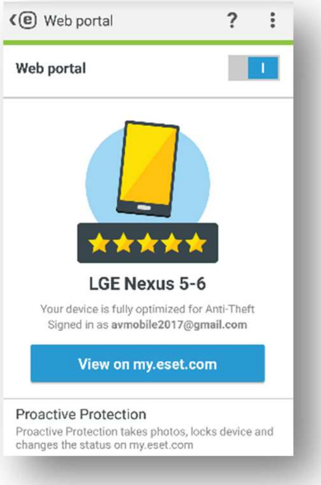

Scheduled scan

Scan running

Package installer

Scan level: In-depth
Type: Scheduled scan
Duration: 00:00:53
Scanned files: 137

No threats found


Web portal

Web portal

LGE Nexus 5-6

Your device is fully optimized for Anti-Theft
Signed in as avmobile2017@gmail.com

Proactive Protection
Proactive Protection takes photos, locks device and changes the status on my.eset.com

Usage

After the initial installation and agreeing to the EULA, the app requires permission to activate ESET Live Grid (a feature that oversees installed apps and gathers security data) and to recognize potentially unwanted applications (PUA). The user next has to specify a preferred email address; setup is then complete, and the 30-day trial of the premium version begins.

Anti-Virus

There are two options provided by the malware scanner: Smart (installed apps and .APK files) or in-depth (all files). The user can upgrade the virus detection modules manually and also choose the server (pre-release or release server) from which signature updates are downloaded. The app also provides real-time protection by scanning files the device is interacting with. Scheduled scans can be set as well as automatically initiated scans. Furthermore, the user can decide if he/she wants to detect potentially unwanted apps and/or potentially unsafe apps.

Anti-Theft

Before the Anti-Theft function is ready to use, a bit of setup is necessary. The user needs to establish a security password, which is required to access the anti-theft feature and provide some contact information that is shown on the lock screen. Furthermore, the app requires admin rights on the phone for Uninstall Protection, and the user can enable the SIM Guard to protect the device against an unauthorized SIM card change. ESET provides an external web interface which allows the remote management of the device. Once the device recognizes suspicious behaviour, it will enter the “suspicious mode”. In this state, the app regularly sends data (photos taken by the front and back camera, device’s location, and information about connected Wi-Fi networks) to the web interface. In addition, the user can activate the "Last known location" feature, where the location is sent to the server when the device battery will reach a critical level. The user can also lock the device from the website with one click, and run an anti-theft test. Recommendations on how to further improve the security level and to configure the device to an even safer state can be found on the website as well as in-app.

Anti-Phishing

The Anti-Phishing feature protects a wide range of browser apps against accessing phishing websites and websites with dangerous content. The user will be notified in case of a detection and can decide if he/she wants to proceed or leave the site. The websites detected as risks will be shown in the threat history.

Security Audit

The user can review and adjust important settings and permissions for the device from inside the app. This feature is split into Device Monitoring (which focuses on different device settings like Wi-Fi, memory, roaming, and installation from unknown sources) and Application Audit, which shows the app permissions granted.

SMS & Call Filter

With this feature, users are able to block incoming and outgoing calls using black- and whitelists, and can set a schedule (times of day and days of the week) when particular numbers should be blocked. When using Android 4.4 or later, the application notifies the user that SMS can't be blocked. In our test, the call filter worked flawlessly, as well as black-/whitelisting different callers.

Conclusion

ESET Mobile Security & Antivirus provides a wide range of different security and anti-virus features with comprehensive settings. All features worked faultlessly and the instructions leave almost no room for questions. If there is still some feature or task that the user does not understand, he/she can look it up in the application's help pages. In conclusion, this app can be recommended to customers who want an easy-to-use product while still being protected well.

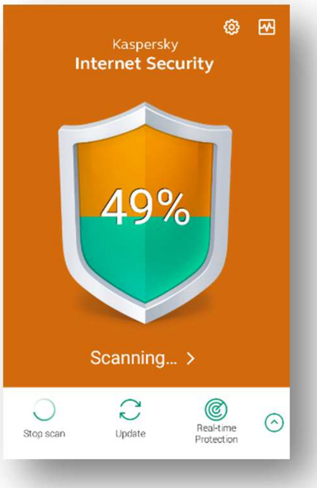
Anti-Theft Details		
Commands Web		
Locate / Track	✓	Displayed on *Google Maps* Map.
Mark as Lost	✓	Triggers device lock. Automatically tracks the phone's position and takes pictures.
Siren	✓	
Lock	✓	Automatically locks the device when marked as lost.
Wipe	✓	Triggers a factory reset and wipes external storage.
Download activity	✓	All the pictures taken and locations can be downloaded as a ZIP archive.
Messages	✓	Allows user to send a single message which is shown as pop-up.
Commands SMS		
Lock	✓	
Siren	✓	
Locate	✓	
Wipe	✓	As for the corresponding web command.
Additional Features		
SIM Guard	✓	Locks the device if (trusted) SIM card is removed or changed.
Uninstall Protection	✓	Locks the device if device administrator rights are removed from the app.
Proactive Theft Protection	✓	Sends an e-mail to the user and regularly data (pictures, location, connected Wi-Fi networks) to the web interface on failed unlock attempts; settings like maximum number of failed attempts and time for correction can be customized in-app.

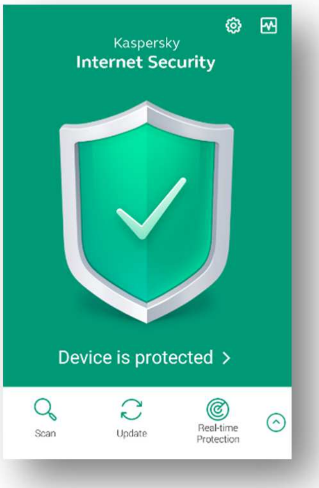
Kaspersky Lab

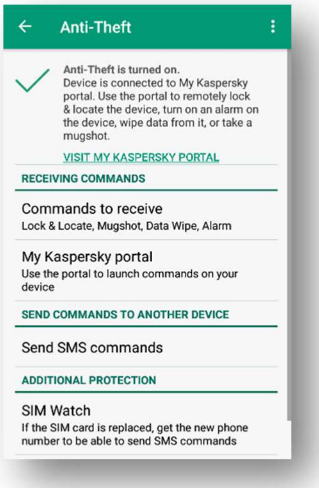
Internet Security
11.14.4

Introduction

Kaspersky Internet Security is an application that not only provides good malware protection but also offers many more important security assets such as theft protection, call blocker, app lock, privacy, and web protection. The user can get the pro version of the app for 10.84€ per year (varies by region).







Anti-Theft is turned on.
Device is connected to My Kaspersky portal. Use the portal to remotely lock & locate the device, turn on an alarm on the device, wipe data from it, or take a mugshot.

VISIT MY KASPERSKY PORTAL

RECEIVING COMMANDS

Commands to receive
Lock & Locate, Mugshot, Data Wipe, Alarm

My Kaspersky portal
Use the portal to launch commands on your device

SEND COMMANDS TO ANOTHER DEVICE

Send SMS commands

ADDITIONAL PROTECTION

SIM Watch
If the SIM card is replaced, get the new phone number to be able to send SMS commands

Usage

On first start-up, the app requests permissions that are necessary for the default configuration and asks the user to accept the EULA. As a final step of the setup, the user may register with *My Kaspersky* in order to properly use all the provided features. After that, an initial scan is started automatically, whereby the user is still able to use the application while it is running.

Anti-Virus

Kaspersky offers to scan either all files, or apps and archives only. Infected files can be moved to quarantine, deleted, or ignored, or the user can be prompted for action. Scheduled scans can be defined and database updates are configured by default to the recommended timetable (with the ability to adjust). When using Real-Time Protection, the user can choose from three settings. "Extended" monitors all actions with files and installed apps. "Recommended" only checks installed apps and installation packages from the Downloads folder. As third option, the real-time protection can be turned off. Users can decide if they want to be protected against potentially unwanted applications too.

Anti-Theft

The app requests some permissions from the user, as well as device admin rights, and wants a secret code to be set before remotely controlling the device. The user can establish a SIM Lock, which locks the device if the SIM is replaced and the device is rebooted. Hot change of SIM will be added in the next version. There is an option to enable/disable receiving the anti-theft commands from the web portal or text messages, these being Lock and Locate, Mugshot, Wipe and Alarm. For the SMS commands to work, the "partner" device also has to have the app installed. All anti-theft commands worked as expected.

Web Protection & Text Anti-Phishing

This feature successfully protects the browser apps installed on the device from malicious and harmful websites. Google Chrome is the only browser that is shown in-app as protected by default. Further tests showed that Boat Browser and Opera Mini are also supported, but these are not mentioned in the product (although this would be useful). Web protection for Firefox and Opera worked imperfectly (test phishing site is accessible but protection page appeared either in a new tab or after a tab switch). The app also offers a Text Anti-Phishing tool that checks incoming text messages for links to malicious and harmful websites which can cause financial or other private data theft.

Privacy Protection & App Lock

When activating this feature, it is possible to hide sensitive contact data and conversation history. Consequently, the sync for the Google account is turned off automatically until the user deactivates the Privacy Protection again. Contacts can also be hidden using a text-message command or the web interface. Furthermore, the App Lock component protects critical apps against unauthorized access. Protected apps can be unlocked using the previously configured secret code.

Call & Text Filter

The Call Blocker is a helpful tool for restricting unwanted phone calls or text messages. Kaspersky states clearly that text-blocking does not work for devices with Android later than 4.4 due to technical limitations. Blocked/allowed numbers can be entered manually or imported from the call and/or text message logs. The component operates similarly to a blacklist or whitelist, and its function can be customized further with several filter settings.

Conclusion

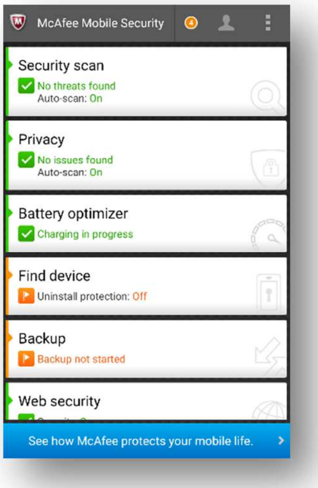
Kaspersky's product provides a great variety of functions and features for mobile security. The fact that there was a brief explanation to every function was very helpful and left no question unanswered. This product is recommended to users who like to keep it simple while also being protected effectively.

Anti-Theft Details		
Commands Web		
Lock & Locate	✓	Displayed on *Google Maps* Map.
Mugshot	✓	Takes several pictures.
Alarm	✓	
Wipe Personal Data	▬	Deletes contacts, text messages, and calendar entries. To completely remove the Google account, the "Wipe All Data" command needs to be executed. External storage is wiped but files can be restored.
Wipe All Data	▬	Triggers a factory reset. External storage is wiped but files can be restored.
Hide Data	✓	Hides contacts listed as sensitive in the Privacy Protection.
Commands SMS		
Alarm	✓	
Locate	✓	
Data Wipe	▬	As for "Wipe Personal Data".
Full Reset	▬	As for "Wipe All Data".
Hide	✓	Hides contact. Reception of command has to be enabled in Privacy Protection.
Additional Features		
SIM Watch	▬	Only locks the device if the SIM is replaced and a reboot is performed.
Uninstall Protection	✓	

McAfee
Mobile Security
4.9.1

Introduction

McAfee Mobile Security comes in a free and a premium version (with a 30-day free trial) and provides components for malware protection, theft protection, privacy control and web security as well as additional features for power/memory management and backups. An upgrade to the premium version includes no ads, 2GB of cloud space and access to the McAfee's premium phone support service.


McAfee Mobile Security

Security scan
No threats found
Auto-scan: On

Privacy
No issues found
Auto-scan: On

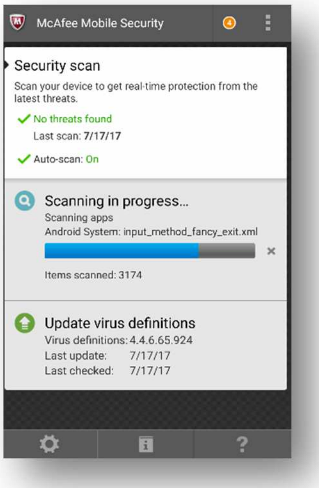
Battery optimizer
Charging in progress

Find device
Uninstall protection: Off

Backup
Backup not started

Web security

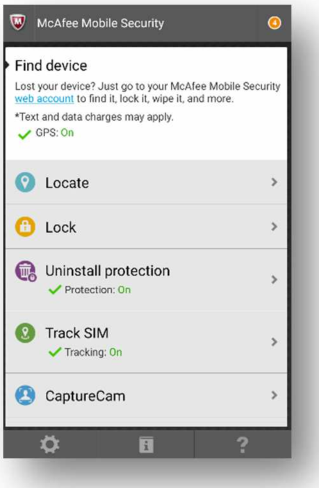
See how McAfee protects your mobile life.


McAfee Mobile Security

Security scan
Scan your device to get real-time protection from the latest threats.
No threats found
Last scan: 7/17/17
Auto-scan: On

Scanning in progress...
Scanning apps
Android System: input_method_fancy_exit.xml
Items scanned: 3174

Update virus definitions
Virus definitions: 4.4.6.65.924
Last update: 7/17/17
Last checked: 7/17/17


McAfee Mobile Security

Find device
Lost your device? Just go to your McAfee Mobile Security web account to find it, lock it, wipe it, and more.
*Text and data charges may apply.
GPS: On

Locate

Lock

Uninstall protection
Protection: On

Track SIM
Tracking: On

CaptureCam

Usage

On the first start up, the app must be granted access to the list of installed apps and the EULA and Privacy Notice have to be accepted. After that, the app runs an initial configuration where the user is asked to turn on the security features by activating McAfee's accessibility service.

Security Scan & Web Security

Users are able to start a scan with pre-defined or custom settings. The scan settings can be adjusted to toggle and schedule real-time scans and automatic updates. Furthermore, the user can decide what should be scanned. This includes apps, potentially unwanted software, text and multimedia messages as well as files in both internal and external storage. An option for turning on/off notifications about malicious apps and files is also available.

In the Web Security component, options for protection against phishing and malware for the browser and to check for risky Wi-Fi connections can be found.

Find Device

When first launching this component, an initial setup is run in order to connect to the web interface. Therefore, a McAfee account and all the necessary permissions for the device is required. The user can create a list of buddies who are notified if the device is lost, stolen or the SIM card is changed. Unfortunately, this feature is not available for EU country users due to EU privacy restrictions. Anti-theft commands can be sent via text messages or a neat web interface. The web interface is basically divided into two parts which makes it a bit confusing: A modern web view "Find device" provides a map and anti-theft commands to react immediately on a lost or stolen device. The legacy page under "My device" or "My data" supports the basic anti-theft commands, further options to wipe and factory reset the device and access the backup data.

Privacy

This feature provides options to check the access to private data for certain apps and restrict or completely lock the access to apps for certain user profiles. The call blocker maintains lists of allowed/blocked incoming and outgoing calls.

Battery Optimizer & Backup

Tools for improving the power and performance of the device are included too. The "Extend Battery" function monitors the battery life and can turn off some power-intensive settings like Bluetooth. A memory cleaner frees up memory from background tasks and a storage cleaner removes unused (cached) data. The component also keeps track of the mobile data usage of the apps over certain time periods.

The app can save private data (text messages, call logs, and contacts) to the cloud and restore this data. It is possible to activate automatic backups or to be notified when there is a new contact or message to back up. In the premium version, it is also possible to backup media files.

Conclusion

McAfee's security product is well-designed and equipped with a comprehensive anti-theft component and additional features to optimize the device's performance and backup data. The anti-theft operations can be triggered via text messages or a web interface. The latter is still split up into two separated pages which is counter-intuitive.

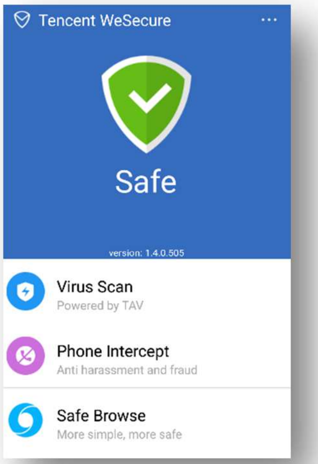
Anti-Theft Details		
Commands Web		
Alarm	✓	Plays one of three device ringtones.
Locate	✓	Displays the device's location on a map.
Lock	✓	Locks the device with or without alarm.
Capture Cam	✓	Plays an alarm, shows a popup message and takes a snapshot of the thief.
I lost my device	✓	Triggers lock, locate and capture cam; if the phone is set to a *lost* state, the additional actions track, backup, wipe and reset can be used.
Track	✓	Tracks the phone for one or six hours continuously.
Backup	✓	Backs up personal data. Backup of media files is only possible in-app.
Wipe	▬	Deletes data on internal and external storage. Latter can be restored.
Reset	✓	Triggers a factory reset; app remains after reset.
Commands SMS		
Alarm	✓	Triggers a fairly realistic screaming alarm tone on the phone.
Locate	✓	Sends a link with a map showing the location.
Lock	▬	The PIN appears in the notifications briefly before locking the screen.
Capture Cam	✓	Triggers the capture cam via a text message.
Wipe	▬	As for the corresponding web command.
Reset	✓	As for the corresponding web command.
Additional Features		
SIM Change Protection	✓	Locks the device and notifies the user via email if the SIM card is removed or changed.
Uninstall Protection	✓	Locks the device if device administrator rights are removed from the app.
Capture Cam	✓	Takes an automatic snapshot when the wrong login credentials are provided for the Android or McAfee lock screen.

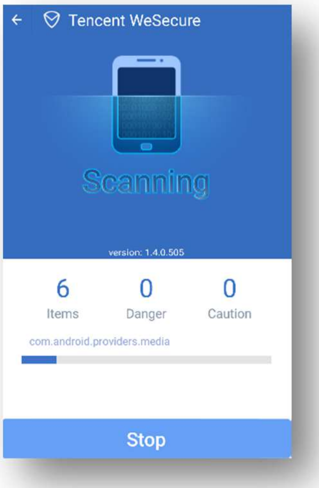
Tencent

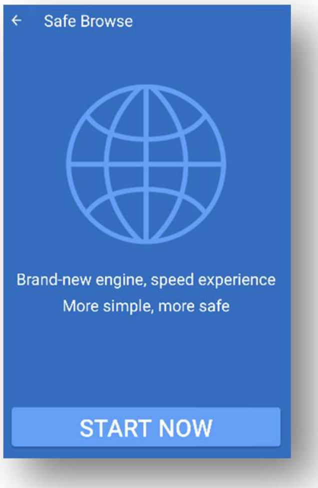
WeSecure
1.4.0

Introduction

Tencent's WeSecure application primarily focuses on malware, protection but also provides external tools for the mobile device, like Safe Browse and Data Backup. Since our last *mobile* test, Tencent have removed the "Phone Accelerator" which was poorly implemented. The app is now simple, completely ad-free, and free of any charges.







Brand-new engine, speed experience
More simple, more safe

Usage

On the first start-up, the user only has to agree to the Terms of Service and Privacy Statement and can continue on to the home screen immediately. It shows the status of the anti-virus component in the form of an icon and text, and all the features provided.

Virus Scan

The user can choose between a "Quick Scan" (scan only installed apps) and a "Full Scan" (scan all files). Both options include a scan of the internal and external storage. If malicious files are found, the user can easily remove them all at once. Automatic updates of the virus database are performed by default.

Phone Intercept

This component enables automatic blocking of fraudulent and harassment calls, using rules applicable to Chinese telephone numbers, and is not customizable.

Safe Browse & Data Backup

The QQBrowser is a safe browser app which has to be downloaded from a third-party source. Therefore, the user must permit this download in the security settings by allowing the installation of apps from unknown sources. The browser requests access to photos, media, files, the location of the device, and at the time of writing only supports Chinese language.

Like the browser app, the Data Backup component is not included in the main app and needs to be downloaded separately. The app itself requires a Tencent QQ account and access to the private data to allow the user to back up contacts, text messages, and call logs.

Conclusion

Tencent WeSecure is a simple, lightweight anti-virus application and offers additional tools which can be downloaded if needed. Tencent users can rely on Android's built-in anti-theft features.

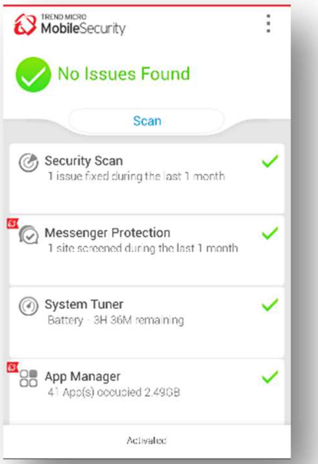
Trend Micro

Mobile Security

8.2.4

Introduction

In addition to malware protection, Trend Micro's product offers several other security features. The app comes in a free and pro version, whereby the pro version has a number of additional features like theft-, network-, and messenger protection as well as the app- and call blocker.



TREND MICRO MobileSecurity

No Issues Found

Scan

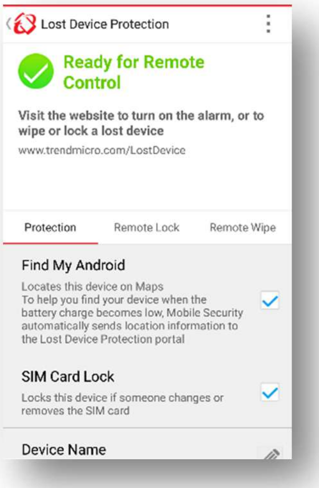
Security Scan ✓
1 issue fixed during the last 1 month

Messenger Protection ✓
1 site screened during the last 1 month

System Tuner ✓
Battery - 3H 36M remaining

App Manager ✓
41 App(s) occupied 2.49GB

Activated



Lost Device Protection

Ready for Remote Control

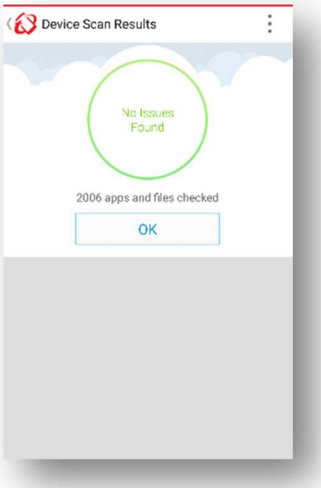
Visit the website to turn on the alarm, or to wipe or lock a lost device
www.trendmicro.com/LostDevice

Protection | Remote Lock | Remote Wipe

Find My Android ☑
Locates this device on Maps
To help you find your device when the battery charge becomes low, Mobile Security automatically sends location information to the Lost Device Protection portal

SIM Card Lock ☑
Locks this device if someone changes or removes the SIM card

Device Name



Device Scan Results

No Issues Found

2006 apps and files checked

OK

Usage

After installing the app and accepting the EULA, the user gets a 7-day free trial of the pro version and is asked to create a Trend Micro account. Afterwards, the app wants permission to send the user-experience to the vendor, in order to provide better protection in the future. The home screen pops up and an initial scan is initiated. The home screen consists of a list of features provided plus the scan and notification area on the top, where missing permissions or threat warnings are displayed.

Security Scan

The user can set the protection to three levels: high, medium, or low. Different scan options like real-time, pre-installation, and SD card scans can be enabled. In the "History" section, scans performed are shown together with database upgrades which are schedulable or manually executable. Any infected app found will be displayed, so the user can decide what should happen next.

Lost Device Protection

This feature is only accessible after entering the account password, and provides the anti-theft functions of the application. The user can enable a SIM card lock, define the message to be shown on the lock screen, and decide if a partial or full wipe should be executed when the wipe command is sent. All anti-theft commands such as alarm, lock, find, and wipe, as well as an option to share the device's location on Facebook, can only be sent from the web interface.

In our tests, we discovered that the web interface didn't support multiple languages for different browsers, which is not very convenient, as most users prefer their native language for their browser. All anti-theft commands and the interactive map only worked properly for browsers set to English. Trend Micro explained that this issue was a leftover of the change from Google Maps to Bing Maps, and they fixed it as soon as we had pointed out.

Network & Messenger Protection

This component provides a safe surfing option, which will inform the user about harmful websites and block them. A Wi-Fi checker is also implemented, which scans the current Wi-Fi network for threats. The protection level is similar to the one in the Security Scan, and is also used for the Messenger Protection, which is very convenient. It can be set to High (block all websites with fraudulent and malicious content), normal (a good balance between protection and accessibility), or low (only block already known harmful websites). The user is able to declare approved or blocked websites and list trusted Wi-Fi networks. The Messenger Protection scans messages in Line and WhatsApp, and warns for malicious links.

Parental Controls

After providing the account password, the user has the opportunity to lock specific apps and inappropriate websites. The website protection is divided into three levels according to the age of a child. Here, the user can also toggle the Uninstall Protection, so Mobile Security can only be removed from the device by entering a password.

Call Blocking

The feature blocks calls effectively, and allows blacklisting and whitelisting of numbers. Optionally, the user can choose the filtering method and the action following a blocked call, e.g. reject and reply with a custom text message.

Additional Features

In addition to the standard security and AV-related components mentioned above, Trend Micro provides System Tuner, which optimizes battery and memory, App Manager, which lists installed applications, and Social Media Scan, which checks the privacy settings for the user's Facebook account.

Conclusion

Trend Micro Mobile Security is made for users who want everything done with one app. With its extensive features, it can provide comprehensive protection. Even though anti-theft commands can be sent easily via the web, text-message commands would be a nice-to-have feature.

Anti-Theft Details

	Commands Web	
Locate / Track	✓	Displayed on a *Bing Maps* map.
Lock	✓	
Full Remote Wipe	━	Triggers a factory reset but external storage is not wiped.
Partial Remote Wipe	✗	Removes only contacts, call logs, and the Trend Micro account which makes future commands impossible. External storage is not wiped.
Alarm	✓	
Share Location on Facebook	✓	Creates a post with a link.
	Additional Features	
SIM Change Protection	✓	Locks the device if the SIM-card is changed or removed; device is unlocked automatically if the original SIM is inserted again.
Uninstall Protection	✓	Part of the Parental Controls component.

Feature List Android Mobile Security (as of July 2017)	*FREE*	FREE	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL
Product Name	*Android OS*	AI Max Dev Labs Security Antivirus - Max Cleaner	Alibaba Ali Money Shield	Avast Mobile Security & Antivirus	Avira Antivirus Security Pro	Bitdefender Mobile Security & Antivirus	ESET Mobile Security & Antivirus	Kaspersky Internet Security	McAfee Mobile Security	Tencent WeSecure	Trend Micro Mobile Security
Version Number	*6.0.1*	1.0	5.5	6.1	5.0	3.2	3.6	11.14	4.9	1.4	8.2
Supported Android versions	*built-in*	4.1 and higher	4.0 and higher	4.1 and higher	4.0 and higher	4.0 and higher	2.3 and higher	4.1 and higher	4.1 and higher	4.2 and higher	4.0 and higher
Supported Program languages	All	Arabic, Chinese, English, French, German, Greek, Indonesian, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish, Thai, Turkish, Ukrainian, Vietnamese	Chinese	Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Malaysian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Spanish, Swedish, Thai, Turkish, Ukrainian, Vietnamese	Dutch, English, French, German, Indonesian, Italian, Japanese, Korean, Polish, Portuguese, Russian, Spanish, Turkish	Czech, Dutch, English, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Thai, Turkish, Vietnamese	Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Kazakh, Korean, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovene, Spanish, Swedish, Thai, Turkish, Vietnamese	English, Russian, German, French, Italian, Spanish, Portuguese, Turkish, Polish, Czech, Danish, Finnish, Hungarian, Norwegian, Dutch, Swedish	Arabic, Bulgarian, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Spanish, Swedish, Thai, Turkish, Vietnamese	English, Chinese	Chinese, Dutch, English, French, German, Hebrew, Italian, Korean, Portuguese, Spanish, Turkish, Vietnamese
Anti-Malware											
On-Install scan of Installed apps	●	●	●	●	●	●	●	●	●	●	●
On-Demand scan	●		●	●	●	●	●	●	●	●	●
On-Access scan for files	●		●	●			●	●	●	●	
Scan works offline		●	●	●	●		●	●	●	●	●
Scan is assisted by cloud	●	●		●	●	●	●	●	●	●	●
Automatic (scheduled) Scan				●			●	●	●	●	●
Scan installed apps for (possible) privacy violations	●	●	●	●		●	●		●	●	●
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●		●	●	●	●	●	●		●
Supported browsers (Safe Browsing)	Google Chrome	Google Chrome	N/A	Amazon Silk, Boat Browser, Dolphin, Firefox, Google Chrome, Opera	Google Chrome	Dolphin, Firefox, Google Chrome, Opera Mini, Opera, Samsung Internet, Facebook Messenger, Facebook	Dolphin, Firefox, Google Chrome, Opera Mini, Opera, Samsung Internet	Boat Browser, Google Chrome, Opera Mini	Google Chrome	N/A	Google Chrome, Samsung Internet
Recommendations for Android settings	●		●				●		●	●	
Quarantine							●	●			
USSD Blocking	●		●	●	●		●	●	●		
Anti-Theft											
Remote Locate, Alarm, Lock & Wipe	●		●	●	●	●	●	●	●	●	●
Webinterface for controlling Anti-Theft features	●		●	●	●	●	●	●	●	●	●
SMS commands for controlling Anti-Theft features				●		●	●	●	●	●	
Notify on SIM Change (Email / SMS)			●	●		●	●	●	●	●	
Lock on SIM Change			●	●			●	●	●	●	●
Remote Unlock			●	●	●		●		●	●	
Anti Spam											
Whitelist / Blacklist Phonecalls		●	●	●	●		●	●	●	●	●
Whitelist / Blacklist SMS			●	●	●		●	●	●	●	●
Whitelist / Blacklist with wildcards				●			●	●	●	●	
Blocking of SMS containing keywords			●					●	●	●	●
Parental Control											
Safe Webbrowsing (content filtering)				●		●			●		●
Lock Apps		●	●	●		●		●	●	●	●
App launcher especially for kids (Parents can choose apps)									●		
Authentication											
Uninstallation protection (password required for uninstallation)				●		●	●	●	●	●	●
Settings protected with password		●		●		●	●	●		●	●
User Account needed to use product	●				●	●		●			●
Additional features											
Backup	●			●					●		●
Local Wipe	●			●				●	●		
Network monitor				●			●		●	●	
Task Killer	●			●					●	●	●
Battery Monitor	●						●		●		●
Support											
Online Help & FAQ	●			●	●	●	●	●	●	●	●
Email support		●	●	●	●	●	●	●	●	●	●
User Forum	●			●	●	●	●	●	●	●	●
User Manual	●		●	●	●	●	●	●	●	●	
Phone Support				●	●	●	●	●	●	●	●
Online Chat						●		●	●	●	
Supported languages of support	All	Chinese, English	Chinese	Chinese, Czech, English, French, German, Italian, Polish, Portuguese, Russian, Spanish, Turkish	Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Malaysian, Portuguese, Russian, Spanish	English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish	All	English, French, German, Italian, Portuguese, Russian, Spanish	Chinese, Czech, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Suomi, Swedish, Turkish	Chinese, English	English
Price (may vary)											
Price 1 Android / 1 year (USD/EUR)	*N/A*	FREE	FREE	USD 8 / 8 EUR	USD 10 / 8 EUR	USD 10 / 10 EUR	USD 15 / 15 EUR	USD 15 / 11 EUR	USD 30 / 30 EUR	FREE	USD 36 / 20 EUR

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (August 2017)